



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/815,518	04/01/2004	David Fultz	IDF 2564 (4000-15700)	8230
28003	7590	09/18/2008		
SPRINT 6391 SPRINT PARKWAY KSOPHT0101-Z2100 OVERLAND PARK, KS 66251-2100			EXAMINER ABEDIN, SHANTO	
			ART UNIT 2136	PAPER NUMBER
			MAIL DATE 09/18/2008	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/815,518	Applicant(s) FULTZ ET AL.	
	Examiner SHANTO M Z ABEDIN	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 03 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 July 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-33 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-33 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 01 April 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 06/09/2008 has been entered.
2. Claims 1-33 are currently presented for the examination.
3. Claims 1-33 have been rejected.

Response to Arguments

4. The applicant's arguments regarding 35 USC 103 (a) type rejections are fully considered, however, moot in view of new grounds of rejection presented in this office action. In particular, upon further consideration, combination of Upton and O'Donnell et al was found to teach the limitations set forth by the arguments (please see below for detail explanations)

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2136

5. Claims 1-3, 9-12, 24, 28 and 29 are rejected under 35 USC 103 (a) as being unpatentable over Upton (US 20030097574 A1) in view of O'Donnell et al (US 2004/0117615 A1)

Regarding claim 1, Upton discloses a system to provide application-to-application enterprise security, the system comprising:

a security application program interface (Fig 4, Fig 5; Par 0051, 0061, 0063, 0069; container; application security services; security provider interfaces) and an application program interface (Fig 4, Fig 5; Par 0061, 0074, 0127; application interfaces) coupled to a client application operable on a first operating system, the security application program interface operable to provide a security credential (Fig 4; Par 0061-0074, 0127-0130; container managed credentials; client application/ interfaces for storing, and providing security credentials);

an authentication authority (Par 0063-0065, 0104, 0128, 0145; SAS, or JAAS, or authentication/ authorization SPI) receiving the security credential (Par 0061-0069; credentials; security-principle; ra.xml file) from the security application program interface, the authentication authority further operable to communicate the token to the security application program interface where the security credential is valid, wherein the token contains user credentials encoded as a platform and application independent string data type (Fig 4; Par 0063-0069, 0104, 0114, 0130, 0150; service provider interface/ SPI; checking public/ password type, or generic/ token type credentials, or security-principal map element).

a store maintaining data validating the security credential (Par 0061-0069; credentials; security-principle; ra.xml file), the store in communication with the authentication authority to validate the security credential (Par 0065-0066; storing credential/ passwords, or ra.xml file);

the application program interface operable to communicating regarding the validating of the token (Par 0061-0074, 0114, 0130, 0150; client application/ interface using credentials/ token for mapping/ authentication) and

a server application operable on a second operating system to receive the token from the application program interface, the server application communicating with the authentication authority to validate the token to enable the client application to use services of the server application (Par 0063-0065, 0104, 0114, 0130; JAAS, or SPI, or 3rd party validating/ authenticating credentials).

Upton fails to disclose expressly the authentication authority further operable to generate a token.

However, Upton's teachings of using, and providing a token as credentials (Par 063-065, 0150, 0065; storing, using token/ credentials, or ra.xml file), suggests enablement of generating the token. Furthermore, O'Donnell et al discloses the authentication authority further operable to generate a token (Par 0061-0070; access/ application server generating, and sending authentication token to user upon validation of the credential). O'Donnell et al further discloses an authentication authority receiving the security credential from the security application program interface, the authentication authority further operable to communicate the token to the security application program interface where the security credential is valid, wherein the token contains user credentials encoded as a platform and application independent primitive data type (Par 0061-0070).

O'Donnell et al and Upton are analogous art because they are from the same field of authentication for network/ enterprise services. At the time of invention, it will be obvious to a person with ordinary skill in the art to combine the teaching of O'Donnell et al with Upton to

Art Unit: 2136

design the system wherein the authentication authority further operable to generate a token in order to facilitate an anonymous token based authentication.

Regarding claim 9, it is rejected applying as same motivation and rationale as applied above rejecting claim 1, furthermore, Upton discloses A method for providing application-to-application enterprise security, the method comprising:

coupling a security application program interface (Fig 4, Fig 5; Par 0051, 0061, 0063, 0069; container; application security services; security provider interfaces) and an application program interface to a client application on a first operating system (Fig 4; Par 0061-0074, 0127-0130; container managed credentials; client application/ interfaces for storing, and providing security credentials);

communicating a security credential from the security application program interface to an authentication authority (Par 0063, 0074, 0127-0130, 0150; client application/ interface providing credentials; 3rd party, or JAAS, or service provider interface/ SPI authenticating public/ password type, or generic/ token type credentials);

communicating information related to the security credential (Par 0061-0069; credentials; security-principle; ra.xml file containing security-principle)between the authentication authority and a data store to determine whether the security credential is valid; wherein the token contains user credentials encoded as a platform and application independent primitive data type (Par 0104, 0114, 0130; service provider interface/ SPI; validating/ authenticating credentials);

communicating the token (Par 0061-0069; credentials; security-principle; ra.xml file containing security-principle) to the client application; providing, by the application program interface coupled to the client application, the token to a server application, the server

Art Unit: 2136

application operable on a second operating system (Par 0061-0074, 0127-0130, 0150; client application/ interface providing credentials; service provider interface/ SPI authenticating public/ password type, or generic/ token type credentials) ; and

validating, by the server application, the token before providing access to services of the server application by the client application (Par 0065-0069, 0104, 0114-0116, 0130; storing credentials, or ra.xml file containing security-principle; SPI, or JAAS, or 3rd party validating/ authenticating credentials).

Upton fails to disclose expressly generating a token by the authentication authority when the security credential is valid.

However, Upton's teachings of using, and providing a token as credentials (Par 063-065, 0150, 0065; storing, using token/ credentials, or ra.xml file), suggests enablement of generating the token. Furthermore, O'Donnell et al discloses the authentication authority further operable to generate a token, wherein the token contains user credentials encoded as a platform and application independent primitive data type (Par 0061-0070; access/ application server generating, and sending authentication token to user upon validation of the credential).

O'Donnell et al further discloses communicating the token to the client application; and validating by the server application, the token before providing access to server application by the client application (Par 0061-0070).

Regarding claim 28, it recites the limitations of claims 1 and 9, therefore, it is rejected applying as above rejecting claim 1 and 9.

Regarding claim 2, Upton discloses the system of Claim 1, wherein the server application further comprises: an application program interface to communicate with the application program interface of the client application (Par 0061-0074, 0127-0130; client application/ interface); and a security application program interface to communicate with the authentication authority (Par 0115, 0128, 0130, 0145, 0147; security services; authentication/ authorization SPI).

Regarding claim 3, Upton discloses wherein the server application is operable to cache the token after validating the token with the authentication authority such that when the client application requests service of the server application, via the application program interfaces of the client application, the server application uses the cached token to validate the client application (Par 0065-0069, 0104, 0114-0116, 0130; storing credentials, or ra.xml file containing security-principle; SPI, or JAAS, or 3rd party validating/ authenticating credentials).

Regarding claims 10-12 and 29, they recite the limitations of claims 1-3, 9 and 28, therefore, they are rejected applying as above rejecting claims 1-3, 9 and 28.

Regarding claim 24, Upton discloses wherein the security credential is further defined as including a password and user identification (Par 0061-0074, 0150).

6. Claims 8 and 15 are rejected under 35 USC 103 (a) as being unpatentable over Upton (US 20030097574 A1) in view of O'Donnell et al (US 2004/0117615 A1) further in view of Laferriere et al (US 2005/0188212 A1).

Regarding claim 8, modified O'Donnell et al -Upton system fails to disclose wherein validating the token by the authentication authority includes determining whether the authentication authority created the token.

However, Laferriere et al discloses wherein validating the token by the authentication authority includes determining whether the authentication authority created the token (Par 0012-0023; claims1,14).

Laferriere et al and Upton are analogous art because they are from the same field of authentication for network/ enterprise services. At the time of invention, it will be obvious to a person with ordinary skill in the art to combine the teaching of Laferriere et al with modified O'Donnell et al - O'Donnell et al -Upton to design the system wherein validating the token by the authentication authority includes determining whether the authentication authority created the token in order to provide credential security through authenticating the credential provider.

Regarding claim 15, it recites the limitations of claim 8 and 9, therefore, it is rejected applying as above rejecting claims 8 and 9.

7. Claims 26-27 are rejected under 35 USC 103 (a) as being unpatentable over Upton (US 20030097574 A1) in view of O'Donnell et al (US 2004/0117615 A1) further in view of Favazza et al (US 20040139319 A1).

Regarding claim 26, although Upton discloses data store is a certificate authority (Par [0076]-[0077]), modified O'Donnell et al -Upton system fails to disclose wherein the security credential is an X.509 certificate.

However, Favazza et al discloses w wherein the security credential is an X.509 certificate (Par 0039, 0050).

Favazza et al and Upton are analogous art because they are from the same field of authentication for network/ enterprise services. At the time of invention, it will be obvious to a person with ordinary skill in the art to combine the teaching of Favazza et al with modified O'Donnell et al -Upton to design the system wherein the security credential is an X.509 certificate to provide alternative secure credentials.

Regarding claim 27, it is rejected applying as above rejecting claim 26, furthermore, Upton discloses communicating the X.509 certificate from the authentication authority to the certificate authority (Par 0073, 0076-0077); validating the certificate by the certificate authority; and communicating validation information to the authentication authority (Par 0073, 0076-0077). Modified O'Donnell et al -Upton system fails to disclose expressly wherein the security credential is an X.509 certificate.

However, Favazza et al discloses wherein the security credential is an X.509 certificate (Par 0039, 0050).

8. Claims 1-7, 9-14, 16-25 and 28-33 are rejected under 35 USC 103 (a) as being unpatentable over Upton (US 20030097574 A1) in view of Bhat et al (US 2003/0200465 A1)

Regarding claim 1, Upton discloses a system to provide application-to-application enterprise security, the system comprising:

a security application program interface (Fig 4, Fig 5; Par 0051, 0061, 0063, 0069; container; application security services; security provider interfaces) and an application program

Art Unit: 2136

interface (Fig 4, Fig 5; Par 0061, 0074, 0127; application interfaces) coupled to a client application operable on a first operating system, the security application program interface operable to provide a security credential (Fig 4; Par 0061-0074, 0127-0130; container managed credentials; client application/ interfaces for storing, and providing security credentials);

an authentication authority (Par 0063-0065, 0104, 0115, 0128, 0145; SAS, or JAAS, or authentication/ authorization SPI) receiving the security credential (Par 0061-0069; credentials; security-principle; ra.xml file) from the security application program interface, the authentication authority further operable to communicate the token to the security application program interface where the security credential is valid, wherein the token contains user credentials encoded as a platform and application independent string data type (Fig 4; Par 0063-0069, 0104, 0114, 0130, 0150; service provider interface/ SPI; checking public/ password type, or generic/ token type credentials, or security-principal map element).

a store maintaining data validating the security credential (Par 0061-0069; credentials; security-principle; ra.xml file), the store in communication with the authentication authority to validate the security credential (Par 0065-0066; storing credential/ passwords, or ra.xml file);

the application program interface operable to communicating regarding the validating of the token (Par 0061-0074, 0104, 0114, 0130, 0150; client application/ interface using credentials/ token for mapping/ authentication) and

a server application operable on a second operating system to receive the token from the application program interface, the server application communicating with the authentication authority to validate the token to enable the client application to use services of the server application (Par 0063-0065, 0104, 0114-0116, 0130; JAAS, or SPI, or 3rd party validating/ authenticating credentials).

Upton fails to disclose expressly the authentication authority further operable to generate a token.

However, Upton's teachings of using, and providing a token as credentials (Par 063-065, 0150, 0065; storing, using token/ credentials, or ra.xml file), suggests enablement of generating the token. Furthermore, Bhat et al discloses the authentication authority further operable to generate a token (Figure 6; Par 0030- 0079; especially Par 0035, 0066, 0077-0079; Claims 1-6; server system having token manager generating token). Bhat et al further discloses an authentication authority receiving the security credential from the security application program interface, the authentication authority further operable to communicate the token to the security application program interface where the security credential is valid, wherein the token contains user credentials encoded as a platform and application independent primitive data type (Par 0030-0079; claims 1-5; especially Par 0077-0079; token including string/ password, user identifying information; sending/ assigning token to application interface to authenticate user for particular application).

Bhat et al and Upton are analogous art because they are from the same field of authentication for network/ enterprise services. At the time of invention, it will be obvious to a person with ordinary skill in the art to combine the teaching of Bhat et al with Upton to design the system wherein the authentication authority further operable to generate a token in order to facilitate an anonymous token based authentication.

Regarding claim 9, it is rejected applying as same motivation and rationale as applied above rejecting claim 1, furthermore, Upton discloses A method for providing application-to-application enterprise security, the method comprising:

coupling a security application program interface (Fig 4, Fig 5; Par 0051, 0061, 0063, 0069; container; application security services; security provider interfaces) and an application program interface to a client application on a first operating system (Fig 4; Par 0061-0074, 0127-0130; container managed credentials; client application/ interfaces for storing, and providing security credentials);

communicating a security credential from the security application program interface to an authentication authority (Par 0063, 0074, 0127-0130, 0150; client application/ interface providing credentials; 3rd party, or JAAS, or service provider interface/ SPI authenticating public/ password type, or generic/ token type credentials);

communicating information related to the security credential (Par 0061-0069; credentials; security-principle; ra.xml file containing security-principle)between the authentication authority and a data store to determine whether the security credential is valid; wherein the token contains user credentials encoded as a platform and application independent primitive data type (Par 0104, 0114, 0130, 0150; service provider interface/ SPI; validating/ authenticating credentials);

communicating the token (Par 0061-0069; credentials; security-principle; ra.xml file containing security-principle) to the client application; providing, by the application program interface coupled to the client application, the token to a server application, the server application operable on a second operating system (Par 0061-0074, 0127-0130, 0150; client application/ interface providing credentials; service provider interface/ SPI authenticating public/ password type, or generic/ token type credentials) ; and

validating, by the server application, the token before providing access to services of the server application by the client application (Par 0065-0069, 0104, 0114, 0130; storing

Art Unit: 2136

credentials, or ra.xml file containing security-principle; SPI, or JAAS, or 3rd party validating/ authenticating credentials).

Upton fails to disclose expressly generating a token by the authentication authority when the security credential is valid.

However, Upton's teachings of using, and providing a token as credentials (Par 063-065, 0150, 0065; storing, using token/ credentials, or ra.xml file), suggests enablement of generating the token. Furthermore, Bhat et al discloses the authentication authority further operable to generate a token, wherein the token contains user credentials encoded as a platform and application independent primitive data type (Par 0031-0078; token)

Regarding claim 28, it recites the limitations of claims 1 and 9, therefore, it is rejected applying as above rejecting claim 1 and 9.

Regarding claim 2, Upton discloses the system of Claim 1, wherein the server application further comprises: an application program interface to communicate with the application program interface of the client application (Par 0061-0074, 0127-0130; client application/ interface); and a security application program interface to communicate with the authentication authority (Par 0115, 0128-0130, 0145-0147; security services; authentication/ authorization SPI).

Regarding claim 3, Upton discloses wherein the server application is operable to cache the token after validating the token with the authentication authority such that when the client application requests service of the server application, via the application program interfaces of

Art Unit: 2136

the client application, the server application uses the cached token to validate the client application (Par 0065-0069, 0104, 0114-0116, 0130; storing credentials, or ra.xml file containing security-principle; SPI, or JAAS, or 3rd party validating/ authenticating credentials).

Regarding claim 4, Upton system fails to disclose wherein the token generated by the authentication authority comprises a string including at least a portion of the security credential.

However, ***Bhat et al*** discloses wherein the token generated by the authentication authority comprises a string including at least a portion of the security credential (Par 0031-0077).

Regarding claim 5 and 6, Bhat et al discloses wherein at least a portion of the token is in Extensible Markup Language format (Par 0030; token as a part of URL; using XML). Furthermore, the examiner takes an official notice on that at the time of invention use of XML for defining credential or token was well known in art. Therefore, it would be obvious to a person of ordinary skill in art to define token in XML format so that it can be used in XML type URL access requests.

Regarding claim 7, Bhat et al discloses wherein the token includes information related to an expiration date of the token (Par 0031-0077).

Regarding claims 10-12 and 29, they recite the limitations of claims 1-3, 9 and 28, therefore, they are rejected applying as above rejecting claims 1-3, 9 and 28.

Art Unit: 2136

Regarding claims 13-14, 16-17, 19 and 21-23, they recite the limitations of claims 4-7 and 9, therefore, they are rejected applying as above rejecting claims 4-7 and 9.

Regarding claim 18, Bhat et al discloses wherein the token includes a portion of the security credential in a string format (Par 0066-0078)

Regarding claim 20, Bhat et al discloses wherein the token is encrypted (Par 0066-0078; encrypted token).

Regarding claim 24, Upton discloses wherein the security credential is further defined as including a password and user identification (Par 0061-0074, 0150). Furthermore, Bhat et al discloses wherein the security credential is further defined as password and user identification (Par 0035, 0066, 0077).

Regarding claim 25, it recites the limitations of claim 20 and 24, therefore, it is rejected applying as above rejecting claims 20 and 24.

Regarding claims 30-33, they recite the limitations of claims 4-7 and 28, therefore, they are rejected applying as above rejecting claims 4-7 and 28.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

Art Unit: 2136

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1, 9 and 28 are rejected under 35 USC 102 (e) as being anticipated by US 7249375 B2 (Bhatia et al).

Regarding claim 1, Bhatia et al teaches a system to provide application-to-application enterprise security, the system comprising:

a security application program interface and an application program interface coupled to a client application on a first operating system, the security application program interface operable to provide a security credential (Fig 1; Col 3, starts at line 6; system including SSO server/ partner interfaces, and client interface);

an authentication authority receiving the security credential from the security application program interface, the authentication authority (Col 3, starts at line 6; SSO servers) further generates a token and communicates the token to the security application program interface where the security credential is valid, wherein the token contains user credentials encoded as a platform and application independent string data type (Fig 3; Col 3, starts at line 16; XML/ security token for authentication);

a store maintaining data validating the security credential, the store in communication with the authentication authority to validate the security credential (Col 3, starts at line 44; generating, and storing tokens);

the application program interface communicating regarding the validity of the token (Fig 3; Col 3, starts at line 16; authenticating security token); and

a server application on a second operating system to receive the token from the application program interface, the server application communicating with the authentication authority to validate the token to enable the client application to use services of the server application (Fig 1, Fig 3; Col 3, starts at line 6; RDBMS application server communicating with the SSO authentication servers).

Regarding claim 28, Bhatia et al teaches a system to provide application-to-application enterprise security, the system comprising:

a first application program interface coupled to a first application on a first operating system (Fig 1; Col 3, starts at line 6; user application program interface);

a first security application program interface coupled to the first application on the first operating system to provide a first security credential (Fig 2; Col 3, starts at line 45; user application services);

a second application program interface coupled to a second application on a second operating system (Fig 1, Fig 3; Col 3, starts at line 6; RDBMS application server);

a second security application program interface coupled to the second application on the second operating system, to provide a second security credential (Fig 2; Col 3, starts at line 45; middle tier, or RDBMS application services);

an authentication authority (Fig 3; Fig 4; Col 3, starts at line 6; SSO server/ partners/ third party) receiving the first and second security credentials from the first and second security application program interfaces, the authentication authority further generating tokens and communicating the tokens to the first and second security application program interfaces where the first and second security credentials are valid, wherein the token contains user credentials

Art Unit: 2136

encoded as a platform and application independent data type (Col 3, starts at line 44; generating, and storing XML/ Authentication tokens);

a store maintaining data validating the first and second security credentials, the store in communication with the authentication authority to validate the first and second security credentials (Col 3, starts at line 44; storing tokens);

the first application program interface communicating regarding tokens (Fig 3; Fig 4; Col 3, starts at line 45); and

the second application program interface receiving the token from the first application program interface, the second security application program interface communicating with the authentication authority to validate the token to enable the first application to use services of the second application and wherein the second application receives the token from the second application program interface, the first security application program interface communicating with the authentication authority to validate the token to enable the second application to use services of the first application (Fig 3; Fig 4; Col 3, starts at line 16; RDBMS application server communicating with the SSO authentication servers) .

Regarding claim 9, it recites the limitations of claims 1 and 28, therefore, it is rejected applying as above applied rejecting claims 1 and 28.

Conclusion

10. **Examiner's note:** Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

11. References have not applied to reject, however found closely related to the claimed invention are:

Silhavy et al (US 2005/0108521 A1) discloses access control in a client (database) application based on client token generated previously by server/ security service.

Aupperle et al (US 2004/0098595 A1) discloses an access control system that utilizes security tokens specific to the users and the applications.

12. A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDONMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin

Examiner, A.U. 2136

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136